1

2

3

4

5

6

7

8

BURSOR & FISHER, P.A.
L. Timothy Fisher (State Bar No. 191626)
Stefan Bogdanovich (State Bar No. 324525)
Joshua B. Glatt (State Bar No. 354064)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ltfisher@bursor.com
        sbogdanovich@bursor.com
        jglatt@bursor.com

9

Attorneys for Plaintiffs

10

11

12

13

14

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA—EASTERN DIVSION

15

16

17

18

19

20

21

22

23

ISIAH SHEPPARD, HILSCIO RIVERA, HELENE LAUZIER-MEYER, and BERNABE BENITEZ, individually and on behalf of all others similarly situated,
 	
                                    Plaintiffs,
 	
    v.
 	
FANTASIA TRADING LLC, and ANKER INNOVATIONS LIMITED, d/b/a eufy
 	
                                    Defendants.
	Case No. 5:23-cv-02407-JGB-E
	
	THIRD AMENDED CLASS ACTION COMPLAINT
	
	JURY TRIAL DEMANDED

24

25

26

27

28

Plaintiffs Isiah Sheppard, Hilscio Rivera, Helene Lauzier-Meyer, and Bernabe Benitez ("Plaintiffs") bring this action on behalf of themselves and all others similarly situated against Defendants Fantasia Trading LLC ("Fantasia") and Anker Innovations Limited ("Anker Innovations") doing business as eufy[1] (collectively, "Defendants"), for violations of Illinois' Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq.* The following allegations are based on their counsel's investigation and upon information and belief, except for allegations concerning Plaintiffs themselves, which are based on personal knowledge.

NATURE OF THE ACTION

1.   Plaintiffs bring this action for damages and other legal and equitable remedies resulting from the illegal actions of Defendants in collecting and storing their and other similarly situated individuals' biometric identifiers without first obtaining informed written consent and failing to develop, maintain, or much less provide a data retention and destruction schedule, in direct violation of BIPA.

2.   The Illinois Legislature has found that "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 ILCS 14/5(c). "For example, social security numbers, when compromised can be changed. Biometric identifiers, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identify theft, and is likely to withdraw from biometric-facilitated transactions." *Id.*

3.   In recognition of these concerns over the security of individuals' biometric identifiers, the Illinois Legislature enacted BIPA, which provides, *inter alia*, that a private entity like Defendants may not obtain and/or possess an

---

[1] Although Defendants sometimes refer to their brand as "eufy" and at other times as "Eufy," defense counsel in this action has consistently referred to the brand as "eufy." For ease of reference, this Complaint shall not capitalize the first letter of the brand name unless quoting another source.

individual's biometric identifiers unless it informs that person in writing that biometric identifiers will be collected or stored. *See* 740 ILCS 14/15(b).

4.   Likewise, BIPA also requires that entities collecting biometric identifiers must publish and make publicly available written retention schedules and guidelines for permanently destroying biometric identifiers collected. *See* 740 ILCS 14/15(a).

5.   In direct violation of each of the foregoing provisions of §§ 15(b) and 15(a) of BIPA, Defendants collected, stored, and used—without providing notice, obtaining informed written consent and without publishing a data retention schedule—the biometric identifiers of Illinois delivery drivers making deliveries to homes using Defendants' home security system.

6.   In November 2022, a security researcher revealed that eufy cameras uploaded images and facial recognition data to Defendants' cloud storage, which is hosted by a third party (Amazon Web Services ("AWS"), a subsidiary of Amazon.com, Inc.), even where the user did not sign up for cloud storage or services.

7.   Defendants eventually conceded that, even for users who did not create a cloud account or agreed to the transmittal of images from their eufy camera to Defendants' cloud storage, such images were nevertheless collected, transmitted, and disseminated to the third-party company that hosts Defendants' cloud storage for consumers, *i.e.* AWS. Defendants eventually admitted that it was sharing these images with AWS in January 2023.

8.   To be sure, BIPA independently prohibits the unconsented collection of biometric identifiers that <u>can be used</u> to distinguish unique individuals. Nothing in the text or the history of the statute gives Defendants a free pass to collect this sensitive data without people's consent simply because Defendants avoid actively using the biometric identifiers they collect to identify individuals, or avoid collecting

those same individuals' names, addresses, or other information to link those

biometric identifiers back to individuals' real-world identities.

9.   BIPA confers on Plaintiffs, and all those similarly situated Illinois

residents who make home deliveries, the right to know of the risks inherently

presented by the collection and storage of their biometric identifiers, like the

geometric scans of their hands or face. Plaintiffs also have a right to know how long

such risks will persist while their biometric identifiers are stored and used by eufy's

AI.

10.   This is particularly concerning because other home security companies

like Google Nest and Wyze do not allow their cameras and doorbells with facial

recognition capabilities to be used in Illinois.[2]

11.   Plaintiffs bring this action to prevent Defendants from further violating

the privacy rights of Illinois delivery drivers and to recover statutory damages for

Defendants' unauthorized collection, storage, and use of their biometric identifiers in

violation of BIPA.

PARTIES

12.   Plaintiff Isiah Sheppard is a resident of Cook County, Illinois. Plaintiff

Sheppard works as an Uber Eats and DoorDash delivery driver who makes deliveries

to customers' homes. As part of Plaintiff Sheppard's regular deliveries process, he

walks to the front door of the customer's residence to make the delivery. On

multiple deliveries, scans of Plaintiff Sheppard's face and/or hands were captured by

eufy's security system. Plaintiff Sheppard has a publicly available Facebook account

searchable by his name and which features photos of himself.

---

[2] Google Store, *Nest Aware*, available at
https://store.google.com/us/product/nest_aware?hl=en-US&pli=1 (last accessed Oct.
18, 2023); Wyze, *How do I set up Friendly Faces?* (July 21, 2023), available at
https://support.wyze.com/hc/en-us/articles/5876322908315-How-do-I-set-up-
Friendly-Faces- (last accessed Oct. 18, 2023).

13.   Plaintiff Hilscio Rivera is a resident of Cook County, Illinois. Plaintiff Rivera works as an Amazon, DoorDash, Postmates, Dispatch, Veho, AxleHire and Roadie delivery driver who makes deliveries to customers' homes. As part of Plaintiff Rivera's regular delivery process, Plaintiff Rivera walks to the front door of the customer's residence to make the delivery. On multiple deliveries, scans of Plaintiff Rivera's face and/or hands were captured by eufy's security system. Plaintiff Rivera has publicly available Facebook and Twitter accounts, searchable by his name and which feature photos of himself.

14.   Plaintiff Helene Lauzier-Meyer is a resident of Sangamon County, Illinois. Plaintiff Lauzier-Meyer works as a DoorDash and Spark delivery driver who makes deliveries to customers' homes. As part of Plaintiff Lauzier-Meyer's regular deliveries process, she walks to the front door of the customer's residence to make the delivery. On multiple occasions, scans of Plaintiff Lauzier-Meyer's face and/or hands were captured by eufy's security system. Plaintiff Lauzier-Meyer has a publicly available Facebook account searchable by her maiden name and which feature images of herself.

15.   Plaintiff Bernabe Benitez is a resident of Lake County, Illinois. Plaintiff Benitez works as an UberEats delivery driver who makes deliveries to customers' homes. As part of Plaintiff Benitez's regular deliveries process, he walks to the front door of the customer's residence to make the delivery. On multiple occasions, scans of Plaintiff Benitez's face and/or hands were captured by eufy's security system. Plaintiff Benitez has publicly available Facebook and TikTok accounts searchable by his last name and which feature images of himself.

16.   Defendant Fantasia Trading LLC is a Delaware corporation with its principal place of business in Ontario, California. Fantasia Trading LLC is Anker Innovations Limited's wholly owned subsidiary and is under the control and direction of its parent, Anker Innovations Limited. Fantasia markets and distributes

various electronic devices and accessories under the brand, Anker, as well as other brands including eufy.

17.   Defendant Anker Innovations Limited ("Anker Innovations") is a Chinese company with its principal place of business at Room 1318-19, Hollywood Plaza, 610 Nathan Road, Mongkok, Kowloon, Hong Kong SAR, People's Republic of China. Anker Innovations designs, manufactures, and distributes the eufy camera products for export and sale throughout the world, including throughout the United States, including Illinois and California. Anker Innovations offers the eufy Security App for use with eufy cameras, including by users in Illinois and California.

18.   eufy is a home security technology brand that offers security cameras supported by high quality video and artificial intelligence ("AI") monitoring. On the eufy website's About Us page, it lists "Anker Innovations" as the company that owns several brands, including eufy.[3] The bottom of the page which contains hyperlinks to various legal documents also lists "Fantasia Trading LLC."[4] eufy's Terms of Service similarly list Defendants Anker Innovations and Fantasia as "affiliated companies" and purport to bind both companies into an agreement with users of the "Eufy Security App and devices, eufy Baby App and devices, eufy Clean App and devices, [and] EufyLife App and devices."[5]

19.   Defendants Anker Innovations and Fantasia (collectively, "Defendants") acted jointly to perpetrate the acts described herein, including in the collection of biometric identifiers and are thus subject to joint and several liability. At all times relevant to the allegations in this matter, each Defendant acted in concert with, within the knowledge and approval of, and/or as the agent of the other

---

[3] eufy, *About Us*, https://www.eufy.com/about?ref=footer (last accessed May 10, 2024).

[4] *Id*.

[5] eufy, *Terms of Service*, https://www.eufy.com/policies/terms-of-service?ref=footer (last accessed May 10, 2024).

1 Defendant within the course and scope of the agency, regarding the acts and

2 omissions alleged.

3 ## **JURISDICTION AND VENUE**

4   20.   This Court has subject matter jurisdiction over this action pursuant to 28

5 U.S.C. § 1332(d) because there are more than 100 class members and the aggregate

6 amount in controversy exceeds $5,000,000.00, exclusive of interest, fees, and costs,

7 and at least one class member is a citizen of a state different from Defendants.

8   21.   This Court has personal jurisdiction over Defendants because Defendant

9 Fantasia Trading LLC has its principal place of business in this district, in Ontario,

10 California.

11   22.   This Court has personal jurisdiction over Defendant Anker Innovations

12 because it purposefully availed itself to California's jurisdiction and purposefully

13 directed its activities in this District by working with Defendant Fantasia Trading,

14 LLC to import, and thereby introduce, its eufy cameras (manufactured overseas) into

15 this District, and working with Fantasia Trading, LLC in this District to thereby

16 distribute, market, and sell the eufy camera products and place them in the stream of

17 commerce (throughout the US and Illinois, in particular) from this District. *See, e.g.,*

18 *Yamashita v. LG Chem, Ltd.,* 62 F. 4th 496, 504 (9th Cir. 2023).

19   23.   Defendant Anker Innovations manufactures its products overseas and

20 imports them into this District where they are then distributed by Fantasia Trading

21 LLC in Ontario, California, in this District. In particular, Defendant Anker

22 Innovations works with Defendant Fantasia Trading, LLC to import all, or virtually

23 all, of its eufy cameras into the United States through the port complex of Los

24 Angeles and Long Beach (together known as the San Pedro Bay Port Complex), in

25 this District.

26

27

28

24.   In fact, according to an aggregator of publicly available bills of lading[6], from 2019 to 2024, Defendant Fantasia Trading recorded 5,607 bills of lading. Fantasia Trading's top U.S. ports of unlading is the San Pedro Bay Port Complex with 5,364 bills of lading, which represents 95.7% of *all* Fantasia's bills of lading during that period.[7]

FANTASIA TRADING LLC TOP US PORTS

Port of Unlading	Total Records	Recent Shipment
Los Angeles, California	3,178	2024-07-26
Long Beach, California	2,186	2024-07-24
Tacoma, Washington	106	2023-11-04
Newark, New Jersey	101	2024-07-10
Seattle, Washington	17	2023-11-11
Oakland, California	11	2022-03-17
Savannah, Georgia	4	2021-09-28
Philadelphia, Pennsylvania	2	2023-01-18
Norfolk, Virginia	1	2022-06-16
Houston, Texas	1	2020-06-23

25.   As shown by one of those bills, Fantasia Trading imported into the Port of Los Angeles a "Camera Brand: Eufy," among other products, shipped from Anker Innovations Limited.[8]

//

//

//

//

---

[6] A bill of lading is "[a] document a carrier or agent gives a shipper to carry the goods. It can be a receipt for cargo that is to be taken to a destination." *Bill of Lading*, Black's Law Dictionary (12th ed. 2024).

[7] ImportInfo, *Company Directory – Fantasia Trading LLC*, available https://www.importinfo.com/fantasia-trading-llc (last accessed August 2, 2024).

[8] *See* Bill of Lading for ONEYHAND36422401, *available* https://www.importinfo.com/manifest/20230818056930 (last accessed August 2, 2024).

Bill of Lading Overview

Master BOL #	ONEYHAND36422401
House BOL #	SXCOHANOE2307270
Manifest Number	000001
Bill Type	House Bill
Carrier Code	SXCO
Voyage #	071E
IMO #	9468293
Vessel Name	SEASPAN ADONIS
Vessel Country	US
Place of Receipt	HAIPHONG
Foreign Port of Lading	YANTIAN CHINA (MAINLAND) (57078)
Port of Unlading	LOS ANGELES, CALIFORNIA (2704)
Port of Destination	
Foreign Port of Destination	
Weight	112 KG
Weight in KG	112 KG
Quantity	12 CTN
Volume	
Record Status	New Record
In-bond Entry Type	
Transportation Mode	Vessel, containerized
Container	DRYU9923573
Commodity Description	CABLE FOR MOBILE PHONE CHARGING BRAND:ANKER HS CODE: 8544422000 CAMERA BRAND:EUFY HS CODE : 8525893000

Shipper / Consignee / Notify Party Details

Available shippers, consignees, and notify parties involved.

Shipper

Shipper Name	ANKER INNOVATIONS LIMITED. C/O BOND
Address Line 1	CORP - HANOI BRANCH - LOT 66 & NO 3
Address Line 2	, 6 ROAD, VSIPBAC NINH INDUSTRIAL P
Address Line 3	ARK, PHU CHAN, TU SON DIST,,VN

Consignee

Consignee Name	FANTASIA TRADING LLC
Address Line 1	5350 ONTARIO MILLS PKWY,SUITE 100,O
Address Line 2	NTARIO,CA 91764, UNITED STATES,ONT
Address Line 3	ARIO, 91764,US

26.   In fact, a search in the database for "Camera" under Fantasia Trading's imported commodities reveals 370 bills of lading. All but six of those 370 bills show imports to the San Pedro Bay Port Complex. Critically, *none* of the remaining six bills that went to other ports refence the eufy brand:

1

2

Bill of Lading Overview

Master BOL #	MAEU212158820
House BOL #	AMZDCN212F97B763
Manifest Number	678880
Bill Type	House Bill
Carrier Code	AMZD
Voyage #	131W
IMO #	
Vessel Name	SAN CHRISTOBAL
Vessel Country	SG
Place of Receipt	CNYTN
Foreign Port of Lading	YANTIAN CHINA (MAINLAND) (57078)
Port of Unlading	SAVANNAH, GEORGIA (1703)
Port of Destination	
Foreign Port of Destination	
Weight	16968 KG
Weight in KG	16,968 KG
Quantity	2144 CTN
Volume	
Record Status	New Record
In-bond Entry Type	
Transportation Mode	Vessel, containerized
Container	CIPU5045453
Commodity Description	CARD READER FOR PC USE CHARGER FOR MOBILE PHONE EARPHONE EXTERNAL BATTERY INTERFACE CONVERTER MULTI HORN WIRELESS SPEAKER PORTABLE PROJECTOR

Bill of Lading Overview

Master BOL #	OOLU2124804970
House BOL #	AMZDCN2163B2D912
Manifest Number	689914
Bill Type	House Bill
Carrier Code	AMZD
Voyage #	027E
IMO #	
Vessel Name	OOCL POLAND
Vessel Country	HK
Place of Receipt	CNYTN
Foreign Port of Lading	YANTIAN CHINA (MAINLAND) (57078)
Port of Unlading	NEWARK, NEW JERSEY (4601)
Port of Destination	
Foreign Port of Destination	
Weight	12663 KG
Weight in KG	12,663 KG
Quantity	1281 CTN
Volume	
Record Status	Amended Record
In-bond Entry Type	
Transportation Mode	Vessel, containerized
Container	CSNU7325820
Commodity Description	CHARGER FOR MOBILE PHONE EARPHONE EXTERNAL BATTERY HUB INTERFACE CONVERTER WIRELESS CHARGER SOUNDCORE POUCH

Bill of Lading Overview

Master BOL #	MAEU211801698
House BOL #	AMZDCN21851167F5
Manifest Number	682134
Bill Type	House Bill
Carrier Code	AMZD
Voyage #	130W
IMO #	
Vessel Name	CLEMENTINE MAERSK
Vessel Country	DK
Place of Receipt	CNYTN
Foreign Port of Lading	YANTIAN CHINA (MAINLAND) (57078)
Port of Unlading	NEWARK, NEW JERSEY (4601)
Port of Destination	
Foreign Port of Destination	
Weight	15874 KG
Weight in KG	15,874 KG
Quantity	1463 CTN
Volume	
Record Status	Amended Record
In-bond Entry Type	
Transportation Mode	Vessel, containerized
Container	MSKU9236414
Commodity Description	CABLE FOR MOBILE PHONE CHARGING INTERFACE CONVERTER WIRELESS CHARGER CHARGING DOCK CARD READER FOR PC USE HUB FINGERPRINT SMART LOCK

Bill of Lading Overview

Master BOL #	MAEU211801501
House BOL #	AMZDCN21B2351B85
Manifest Number	682134
Bill Type	House Bill
Carrier Code	AMZD
Voyage #	130W
IMO #	
Vessel Name	CLEMENTINE MAERSK
Vessel Country	DK
Place of Receipt	CNYTN
Foreign Port of Lading	YANTIAN CHINA (MAINLAND) (57078)
Port of Unlading	NEWARK, NEW JERSEY (4601)
Port of Destination	
Foreign Port of Destination	
Weight	12329 KG
Weight in KG	12,329 KG
Quantity	1261 CTN
Volume	
Record Status	Amended Record
In-bond Entry Type	
Transportation Mode	Vessel, containerized
Container	HASU4514302
Commodity Description	FINGERPRINT SMART LOCK MONITOR CAMERA ROBOTIC VACUUM CLEANER WIFI BRIDGE CHARGER FOR MOBILE PHONE PORTABLE PROJECTOR CHARGER FOR EXTERNAL BATTERY

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

Bill of Lading Overview

Master BOL #	MAEU212109388
House BOL #	AMZDCN2153470645
Manifest Number	685215
Bill Type	House Bill
Carrier Code	AMZD
Voyage #	004N
IMO #	
Vessel Name	SEADREAM
Vessel Country	MT
Place of Receipt	CNYTN
Foreign Port of Lading	YANTIAN CHINA (MAINLAND) (57078)
Port of Unlading	SEATTLE, WASHINGTON (3001)
Port of Destination	
Foreign Port of Destination	
Weight	10026 KG
Weight in KG	10,026 KG
Quantity	1098 CTN
Volume	
Record Status	Amended Record
In-bond Entry Type	
Transportation Mode	Vessel, containerized
Container	MRKU6054564
Commodity Description	PROJECTOR STAND ROBOTIC VACUUM CLEANER FLOODLIGHT CAMERA PORTABLE SCREEN

Bill of Lading Overview

Master BOL #	ONEYYGNA12141400
House BOL #	EIHKGSZS20100243
Manifest Number	000001
Bill Type	House Bill
Carrier Code	EIHK
Voyage #	011E
IMO #	9805477
Vessel Name	ONE MINATO
Vessel Country	JP
Place of Receipt	YANGON
Foreign Port of Lading	SINGAPORE SINGAPORE (55976)
Port of Unlading	NEWARK, NEW JERSEY (4601)
Port of Destination	
Foreign Port of Destination	
Weight	2239 KG
Weight in KG	2,239 KG
Quantity	175 CTN
Volume	CM
Record Status	New Record
In-bond Entry Type	
Transportation Mode	Vessel, containerized
Container	TCKU3443507
Commodity Description	MONITOR CAMERA SUIT

THIRD AMENDED CLASS ACTION COMPLAINT
CASE NO. 5:23-CV-02407-JGB-E

11

27.   As such, from the Ports of Los Angeles and Long Beach, Anker
Innovations works with Defendant Fantasia Trading, LLC to have *all* its eufy
cameras distributed and shipped from their Ontario, California distribution center(s)
in this District to and throughout the United States, including Illinois.

28.   In short, all, or at least the vast majority, of the specific eufy cameras
that collected facial geometry scans of each of the Plaintiffs' faces in Illinois were
first manufactured overseas by Anker and imported through the Ports of Los Angeles
and Long Beach, in this District. But for the Ports of Los Angeles and Long Beach,
the eufy cameras that ended up collecting Plaintiffs' facial geometry scans would
have never ended up in the Illinois and would have never ended up forming the basis
of Plaintiffs' claims.

29.   Venue is proper in this District pursuant to 28 U.S.C. § 1391 because
Defendant Fantasia Trading LLC is at home in this District. Venue is proper in this
District pursuant to 28 U.S.C. § 1391 because Defendant Anker Innovations
transacts business in this District, and intentionally availed itself to the laws and
markets within this District.

FACTUAL ALLEGATIONS

I.   eufy's Home Security System, Local AI and BionicMind AI.

30.   The eufy brand is sold, marketed, and distributed by Anker Innovations
throughout the United States. Defendants market, distribute, and sell their "eufy"
branded camera products throughout the United States. Consumers can purchase
these products online, either directly through Anker Defendants or another online
retailer, or at brick-and-mortar stores like Best Buy. These camera products are
specifically marketed for home security, allowing consumers to view live and
recorded video of the areas around their homes and to automatically receive
notifications on their cell phone, tablet, or computer regarding activity detected by
the cameras, including thumbnail images when a person is detected in the cameras'
field of view.

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

31.   The eufy brand is an emerging leader in home security systems. However, eufy "isn't like your traditional alarm company. It's a tech company first[.]"[9]

32.   To that end, eufy sells 17 different security camera models, available in 36 different configurations, all of which come equipped with on-device AI monitoring capabilities.[10] These cameras include multiple models of doorbell cameras, exterior mounted and floodlight cameras, and a series of base stations.[11]

33.   eufy's AI technology is categorized as either "Local AI" or "BionicMind AI." Together, they offer homeowners several different detection features depending on the user's subscription and base station.

34.   "Local AI" (eufy's on-device AI mechanism) uses an "embedded AI chip" built into the cameras which provides "local, safe, and intelligent detection."[12]

35.   The "BionicMind AI" system "has the ability to recognize familiar faces, body shapes/positions, different objects, and even human behavior with its machine self-learning system."[13] The system conducts this analysis "locally on the base station"[14] and is added to an already operating eufy system by incorporating the proper base station. The BionicMind system enables eufy cameras to differentiate between known individuals and strangers by recognizing biometric identifiers (*i.e.,*

---

[9] Aliza Vigderman & Gabe Turner, *eufy Security System Review and Cost*, Security.org (Oct. 12, 2023) *available* https://www.security.org/home-security-systems/eufy/ (last accessed May 8, 2024).

[10] eufy, *AI Features for eufySecurity Devices*, available https://support.eufy.com/s/article/AI-Features-for-eufySecurity-Devices (last accessed May 8, 2024).

[11] *Id.*

[12] *Id.*

[13] Jared Locke, *eufy's Latest Edge Security System Features Self-Learning AI to Identify Family and Friands*, 9To5 Toys (Sep. 30, 2022) *available* https://9to5toys.com/2022/09/30/eufy-edge-security-system-launch/ (last accessed May 8, 2024).

[14] *Id.*

---

1   details about the face's geometry as determined by facial points and contours) and

2   comparing the resulting "face templates" (or "faceprint") against the face templates

3   stored in a database.

4   36.   eufy's intelligent detection arises through six unique features: (1) a

5   human detection feature where the system tries "to detect objects similar to the

6   human shape and filter out other objects like cars and animals for motion alerts;" (2)

7   facial detection where the system tries to "detect and screen faces shown in the video

8   image;" (3) human facial recognition where the system tries to "recognize faces in

9   the video image and identify the person for [the homeowner];" (4) pet detection

10   where the system tries "to detect pets which appear in the video image;" (5) crying

11   detection where the system tries "to detect crying and will notify [the homeowner] if

12   necessary;" and (6) vehicle detection where the system "will catch up with the user's

13   vehicle in the backyard or driveway."[15]

14   37.   Generally, the kind of base station the homeowner uses impacts which

15   version of eufy's AI the homeowner can turn on. For example, the base level

16   "Original HomeBase" allows all AI-incorporated cameras and battery-operated video

17   doorbells to use the human detection and facial recognition features. The

18   "HomeBase 3", alternatively, allows the homeowner to deploy each AI recognition

19   feature. "HomeBase E" and "HomeBase 2" allow the homeowner to use just the

20   Human Detection and Facial Recognition detection features.[16]

21   38.   Although the homeowner has, in some instances, a choice of *which* base

22   station to pair with their eufy camera, "eufyCam (eufyCam [,] eufyCam E [,]

23   eufyCam 2 [,] eufyCam 2C [,] eufyCam 2 Pro [,] eufyCam 2C Pro) *must* be used

24

25

26

_____

27   [15] eufy, *supra* note 9.

28   [16] *Id*.

_____

THIRD AMENDED CLASS ACTION COMPLAINT   14
CASE NO. 5:23-CV-02407-JGB-E

with HomeBase[,]"[17] thereby ensuring that eufyCam and eufyCam2 cameras are AI-

capable. Likewise, the eufyCam 3 comes included with the HomeBase3.[18]

      39.   However, unlike the rest, eufy's *wired* video doorbells allow the

homeowner to use the human and facial detection features without needing a base

station.[19]

      40.   Regardless of which camera is used, eufy's Local AI system is

remarkably accurate. As eufy boasts, its on-camera AI human detection feature

"accurately detect[s] humans and vehicles" 95% of the time.[20]

Likewise, users can enhance their system's AI capabilities by adding eufy's

BionicMind AI-equipped base stations to their security systems.[21] eufy's

---

[17] eufy, *Does eufyCam Have to be Used with HomeBase?* available
https://support.eufy.com/s/article/Does-eufy-cameras-have-to-be-used-with-
HomeBase (last accessed May 8, 2024) (emphasis added).

[18] Cool Blue, *What are the Differences Between the EufyCam 3, 2 Pro, and 2?*
available https://www.coolblue.nl/en/advice/compare-the-eufycam-3-with-the-2-pro-
and-2.html (last accessed May 8, 2024).

[19] eufy, *supra* note 9.

[20] eufy, *SoloCam S340*, available https://www.eufy.com/solocam-
s340?utm_source=google&utm_medium=search&utm_content=alwayson&utm_cam
paign=us_security_edge_conversion_search_eufycam_purchase_ost_M3_bb&utm_t
erm=19626718763_144313519606_676641948951&gclid=CjwKCAjwvrOpBhBdEi
wAR58-
3NdpFPlGlnThHvpGuSIhMB31i0N0GkYya92NvW0IIXAjSnobXtGefBoCVVoQA
vD_BwE (last accessed May 8, 2024).

[21] *See* Jennifer Pattison Tuohy, *eufy's Impressive New Smart Cameras Use AI to
Identify You and Your Pets*, The Verge (Sep. 30, 2022) *available*

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

BionicMind AI system, which can be added simply by connecting a new base station,[22] "uses self-learning algorithms after every facial and body shape scan to improve recognition accuracy to more than 99.9% over time—no matter what [the subject is] wearing and how [the subject] approach[es] the camera."[23]

Self-Learning Facial Recognition

BionicMind™ uses self-learning algorithms after every facial and body shape scan to improve recognition accuracy to more than 99.9% over time—no matter what you're wearing or how you approach the camera.

41.   Human detection, available for "Local AI" and "BionicMind AI" users, "detects and captures motion . . . for accurate object classification."[24]

---

https://www.theverge.com/2022/9/29/23378472/eufy-homebase-3-eufycam-3-price-release-date-specs (last accessed May 8, 2024).

[22] *See* eufy, *supra* note 19. ("HomeBase 3 has expandable local storage up to 16 TB, while adding the power of BionicMind for an accurate AI experience.")

[23] eufy, *eufyCam 3*, *available* https://us.eufy.com/pages/security-eufycam3 (last accessed May 8, 2024).

[24] eufy, *How Does the Human Detection Technology Work?* available https://support.eufy.com/s/article/How-does-the-Human-Detection-technology-work (last accessed May 8, 2024).

42.   The technology "works in two steps[.]"[25] First, "[w]hen the camera detects motion in its field of view, the AI engine analyzes the figure to determine if it is a human being or not."[26] Second, "if the captured face meets the AI engine's analysis parameters, the AI engine will try to capture the face and then send a notification to the user."[27] This step allows the system to use the captured biometric identifiers in two scenarios.

43.   One such feature is "cross camera tracking" where, once stored with the proper base station connected, eufy's system will "automatically compile shots **of the same event and person** and organize them chronologically into a single clip"[28] if an event occurs within the view of multiple cameras.

---

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] Anthony Spadafora, *Eufy's New Security Cameras Use AI for Cross-Camera Tracking—Here's How it Works*, Yahoo! Tech (Sep. 26, 2023) *available* https://finance.yahoo.com/news/eufy-security-cameras-ai-cross-230048637.html. (last accessed May 8, 2024) (emphasis added).
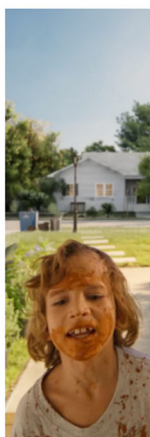
Cross Camera* Tracking

Automatically splice together videos of the same event or person, in order of occurrence, across cameras*. Creates a coherent event video allowing you to quickly and comprehensively understand events completely.
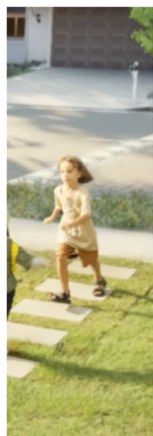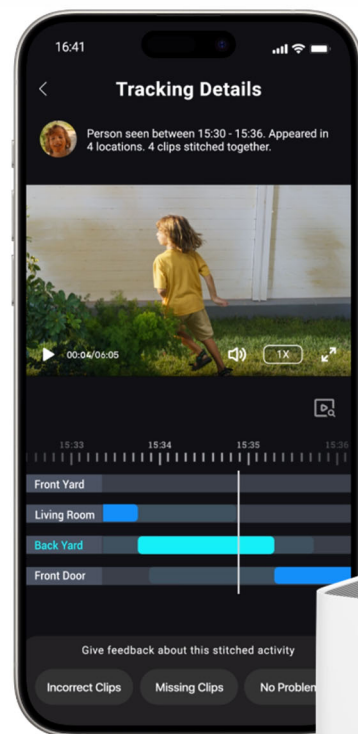
Captured on SoloCam S340
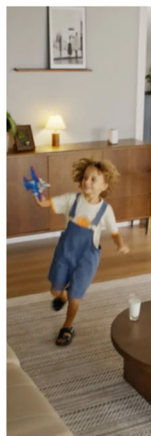
Captured on Indoor Cam S350

Captured on Video Doorbell E340

Captured on Floodlight Cam E340

44.   As eufy explains, "[w]hen the same individual appears across multiple cameras within a specified timeframe, the system automatically locates and merges these footage [sic] into a single video" so that the homeowner can "easily review the entire activity **of that specific individual** in a single video."[29]

45.   To piece the footage together, the BionicMind base station "analyzes the video content and stitches it together in-real [sic]" time and, "[a]fter each camera has finished recording and saving videos to [the base station], [] re-analyzes the video content for splicing."[30] Cameras that are not compatible with BionicMind base

---

[29] eufy Support, *Introducing the Cross-Camera Tracking Function in the eufy Security App*, eufy *available* https://support.eufy.com/s/article/Introducing-the-Cross-Camera-Tracking-Function-in-the-eufy-Security-App (last accessed May 8, 2024) (emphasis added).

[30] *Id.*

THIRD AMENDED CLASS ACTION COMPLAINT   18
CASE NO. 5:23-CV-02407-JGB-E

stations cannot stitch images together in real time and, instead, analyze saved video after recording has ended.[31]

46.   The homeowner then receives a notification alerting them that the device has either detected an already cataloged face like a friend or a new, unknown visitor like a delivery driver:

07:10 AM, seen a person activity.

Appeared in 2 locations.
12 clips stitched together.
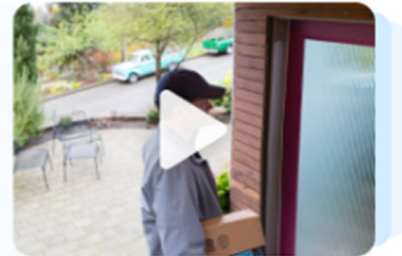
When multiple individuals appear at the same time, a separate event will be created for each individual.
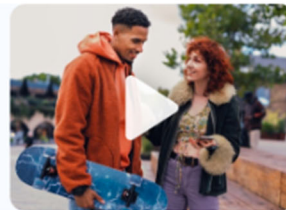
08:30 AM, seen their appearing together.

Robert
Appeared in 2 locations.
12 clips stitched together.

Lia
Appeared in 2 locations.
12 clips stitched together.

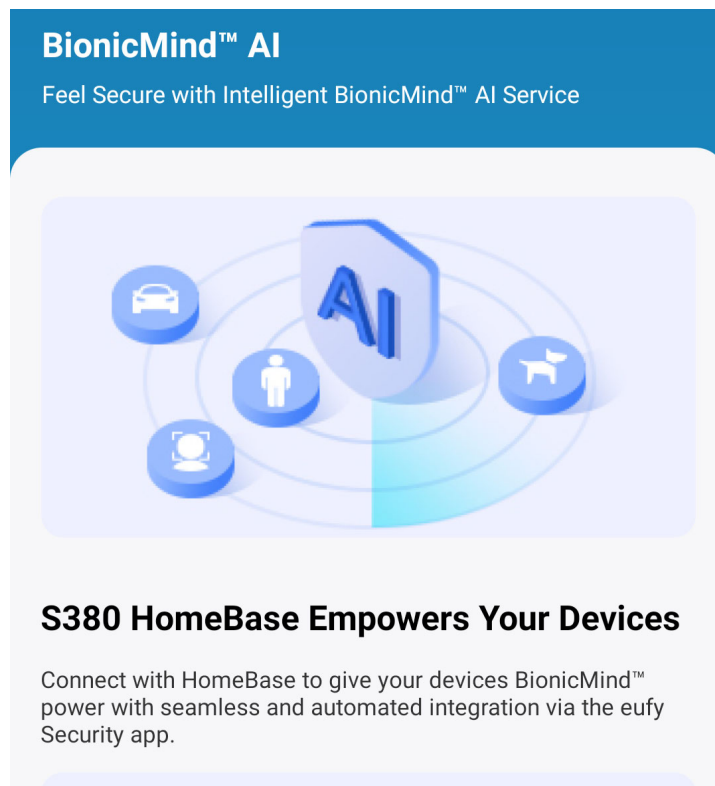47.   eufy is capable of making these identifications by storing and analyzing biometric-identifier data so the AI can "keep learning the details of the characteristics of people, including different angles of the face and bodies" to "help

---

[31] *See Id.* ("Cameras that are compatible with HomeBase 3 storage, but not with HomeBase 3 BionicMind [] A.I., will only be able to use the Look-Back Tracking Function. . .").

1   the AI recognize a person more accurately and quickly."[32] That data is then

2   accessible to the user via the eufy Security App.[33]

3   48.   eufy, through its marketing, actively invites users to take advantage of

4   its BionicMind AI feature, thereby enabling collection and capture of biometric

5   identifiers, as shown by a screenshot posted to a eufy community forum page by a

6   eufy camera user.[34]

BionicMind™ AI

Feel Secure with Intelligent BionicMind™ AI Service

S380 HomeBase Empowers Your Devices

Connect with HomeBase to give your devices BionicMind™
power with seamless and automated integration via the eufy
Security app.

20   49.   In marketing the service, eufy encourages its users to "[c]onnect with

21   HomeBase to give your devices BionicMind power with seamless and automated

22   integration via the eufy Security app."

---

[32] eufy Support, *What is the self-learning AI in the HomeBase 3?* eufy (Dec. 1, 2022)
available https://support.myeufy.com.au/support/solutions/articles/73000597074-
what-is-the-self-learning-ai-in-homebase-3- (last accessed May 8, 2024).

[33] *Id.*

[34] eufy, *Please Empower All Paired Cameras with BionicMind*, available
https://community.security.eufy.com/t/please-empower-all-paired-cameras-with-
bionicmind/3724469/2 (last accessed May 2, 2024).

THIRD AMENDED CLASS ACTION COMPLAINT   20
CASE NO. 5:23-CV-02407-JGB-E

## II.   The eufy Security App and Defendants' Data Storage Practices

50.   The cameras' labels advertise and warrant that "[a]ll your footage is securely stored locally[,] [e]nsuring the videos you record are for you and only you." However, this was not the case.

51.   Consumers who purchase a eufy camera must use the eufy Security App smartphone application. The eufy Security App allows users to access their cameras, view live and historical video feeds, and adjust the cameras' settings. The cameras communicate with the eufy Security App to provide users notifications, such as when the camera detects activity.[35] As referenced above, the eufy cameras communicate with the eufy Security App to provide user notifications, such as notification of activity on the cameras.

52.   The eufy App also allows users to access and review specific data points such as scanned faces (*i.e.,* biometric identifiers):

//

//

//

//

//

//

//

//

//

//

//

//

---

[35] Google Play, *eufy Security*, available https://play.google.com/store/apps/details?id=com.oceanwing.battery.cam&hl=en_US&gl=US (last accessed Apr. 30, 2024).

THIRD AMENDED CLASS ACTION COMPLAINT   21
CASE NO. 5:23-CV-02407-JGB-E
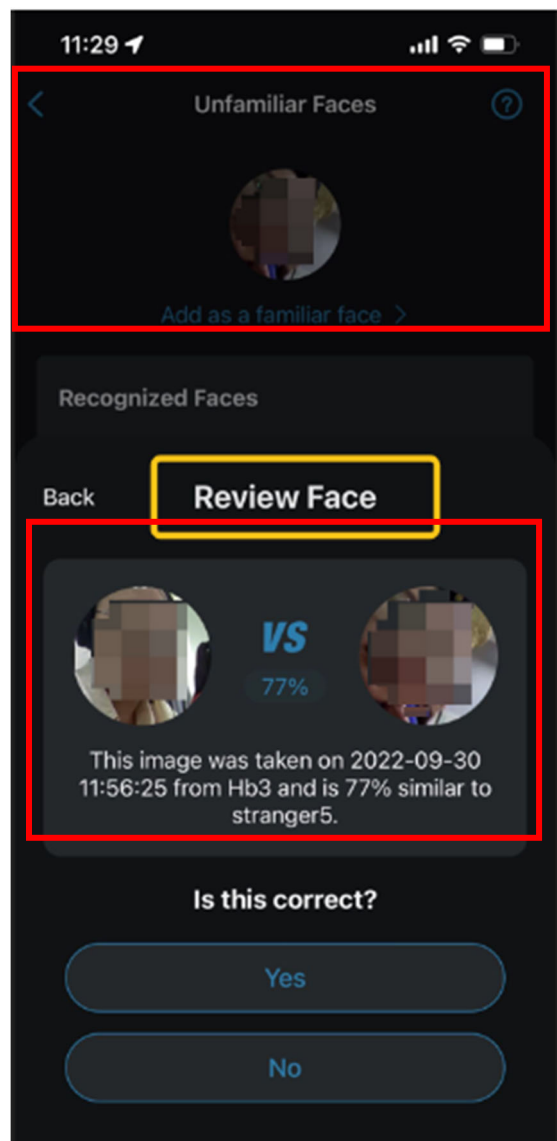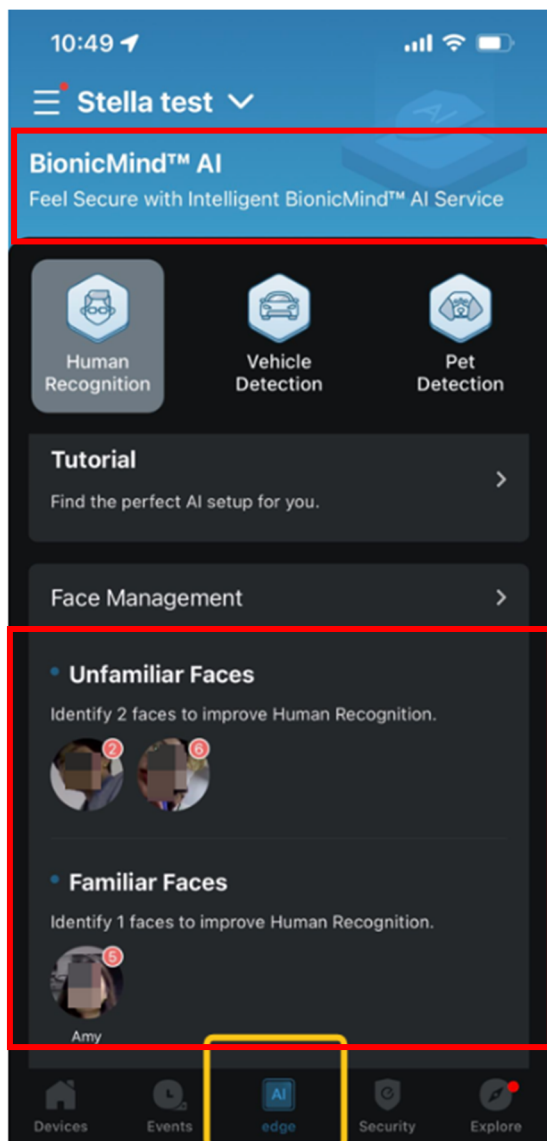
53.   Ensuring that its products have access to biometric identifiers is critical to some of eufy's marketed features. In fact, eufy readily admits that "[t]he Cross-Camera Tracking function depends on a human feature recognition algorithm [sic] that determines the similarity of an individual's appearance in two videos to stitch them together. Even if the face is not visible in the video, videos of similar-looking individuals are still identified and stitched together."[36]

---

[36] eufy, *supra* note 28.

54.   And, although eufy represents that its AI and biometric collections are stored locally, as recently as December 2022 (well within BIPA's five-year statute of limitations from the commencement of this action), "it was revealed that Anker's eufy was sending data from its cameras to the cloud, despite" [37] advertising "several of its security cameras with the promise that video footage and other data are local only."[38] eufy marketed that "its cameras and video doorbells [used] local-only recording for enhanced security, but a security researcher found that the company was uploading images from the cameras to AWS servers alongside facial recognition data.[39] Specifically, the researcher, in testing one of eufy's devices, found that "[t]he doorbell's camera was uploading facial recognition data from the camera to Eufy's cloud servers with identifiable information attached, and that this data wasn't actually removed from Eufy's servers when the related footage had been deleted from the Eufy app."[40] The researcher, in making this discovery, also expressed concern that "Eufy could link footage collected from different cameras and apps to individuals using facial recognition."[41]

---

[37] Ben Schoon, *Eufy Will Add a Disclosure to its App Following Security Concerns but Still Denies Glaring Security Holes,* 9to5Google (Dec. 5, 2022) *available* https://9to5google.com/2022/12/05/eufy-disclosure-cloud/ (last accessed May 8, 2024).

[38] Ben Schoon, *Eufy Caught Lying About Local-Only Security Cameras with Footage Sent to Cloud, Accessible in Unencrypted Streams*, 9to5Google (Dec. 1, 2022) *available* https://9to5google.com/2022/12/01/eufy-camera-cloud-security-leak/ (last accessed May 8, 2024).

[39] Ben Schoon, *supra* note 36.

[40] Ben Schoon, *supra* note 37.

[41] Joel R. McConvey, *Eufy Doorbell Cameras Uploading Facial Recognition Data to the Cloud Without Consent*, Biometric Update (Nov. 30, 2022) *available* https://www.biometricupdate.com/202211/eufy-doorbell-cameras-uploading-facial-recognition-data-to-the-cloud-without-consent (last accessed May 8, 2024).

---

55.   AWS Servers are servers offered by Amazon.com to companies like Defendants as "low-cost ways to deliver their websites and web applications" to users.[42]

56.   That researcher's findings were supported by security firm SEC Consult who summarized two years of analyzing a eufyCam, noting a similar transfer of thumbnails through a cloud service. The company also saw the weak keys, suggesting "hard-coded encryption/decryption keys which are *identical for all sold Homebase devices*," though it was unclear for what the keys were being used.[43]

57.   The data wrongfully collected, transmitted, and disseminated by Defendants includes biometric identifiers. One of the most prevalent uses of biometric identifiers is in facial recognition technology, which works by scanning a human face or an image thereof, extracting facial feature data based on specific identifiers, and comparing the resulting "face template" (or "faceprint") against templates stored in a database.

58.   In fact, once this and other reckless data management practices were discovered, eufy acknowledged in a January 2023 press release that "[p]reviously, we [had] one device, the Video Doorbell Dual, that sent and stored an image of the user to our secure cloud … First, the purpose of sending a user image from the eufy App to our devices is to give the local facial recognition software a baseline to run its

---

[42] *See* Amazon Web Service, *AWS*, available https://aws.amazon.com/free/webapps/?gclid=Cj0KCQiA2eKtBhDcARIsAEGTG42 H9ebgefFKYVCD5h-YNFJ39VpoUAvyk1r0DUwhVMIM-iwBVJph6noaAsOaEALw_wcB&trk=0859629e-29af-428f-ab68-152ecf240a0b&sc_channel=ps&ef_id=Cj0KCQiA2eKtBhDcARIsAEGTG42H9ebge fFKYVCD5h-YNFJ39VpoUAvyk1r0DUwhVMIM-iwBVJph6noaAsOaEALw_wcB:G:s&s_kwcid=AL!4422!3!531871356653!p!!g!!aw s%20web%20hosting!11086666988!111455470529 (last accessed May 8, 2024).

[43] SEC Consult, *The eufyCam Long-Term Observation*, SEC CONSULT (Nov. 24, 2022), *available* https://sec-consult.com/blog/detail/the-eufycam-long-term-observation/ (last accessed May 3, 2024) (emphasis added).

---

algorithm."[44] However, as would be revealed, Defendants' storing facial thumbnails in its cloud was actually occurring across *all eufy devices* and such external storage was necessary to allow eufy Security App users to receive push notifications with faces. "[T]hese thumbnails [were] temporarily sent to Eufy's AWS servers before arriving in [a eufy Security App] notification."[45]

59.   After this revelation, Defendants stated that they were "revising the push notifications option language in the eufy Security app to clearly detail that push notifications with thumbnails require preview images that will be temporarily stored in the cloud."[46, 47]

---

[44] Sean Hollister, *Anker Finally Comes Clean About Its Eufy Security Cameras*, The Verge (Jan. 31, 2023) *available* https://www.theverge.com/23573362/anker-eufy-security-camera-answers-encryption (May 8, 2024) (Emphasis added).

[45] Christopher Boyd, *eufy "No Cloud" Security Cameras Streaming Data to the Cloud*, MALWAREBYTES LABS (Dec. 5, 2022) *available* https://www.malwarebytes.com/blog/news/2022/12/is-your-home-security-system-storing-data-100-locally#:~:text=%E2%80%9CWe%20are%20revising%20the%20push,consumer%2Dfacing%20marketing%20materials.%E2%80%9D (last accessed Apr. 30, 2024).

[46] *Id.*

[47] Amazon.com, *eufy Security Indoor Cam E220, Pan & Tilt, Indoor Security Camera, 2K -3 MP Wi-Fi Plug-In, Voice Assistant Compatibility, Night Vision, Motion Tracking, HomeBase 3 Compatible, Motion Only Alert*, available https://www.amazon.com/eufy-Security-Assistant-Compatibility-Tracking/dp/B0856W45VL (last accessed May 8, 2024).

THIRD AMENDED CLASS ACTION COMPLAINT   25
CASE NO. 5:23-CV-02407-JGB-E

60.   Defendants were aware of the transmissions. Defendants specifically designed and manufactured the cameras to communicate data, over the internet, often to Defendants' own servers and with its security app. Despite Defendants' exclusive knowledge regarding the design and operation of the cameras, the AI, its App, and cloud servers, Defendants continued to market the cameras as only storing data locally. It wasn't until third-party security experts examined the cameras and published their results that Defendants were forced to address these transmissions.

61.   Indeed, the Illinois Legislature was motivated to enact BIPA to protect unauthorized disclosure of biometric identifiers because "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 ILCS 14/5(c). Accordingly, because "[b]iometrics [] are biologically unique to the individual [,] once compromised, the individual has no recourse, is at heightened risk for identify theft, and is likely to withdraw from biometric-facilitated transactions." *Id.*

62.   Due to these concerns, BIPA provides, *inter alia*, that private entities like Defendants may not obtain and/or possess an individual's biometric identifiers unless it informs that person in writing that biometric identifiers will be collected or stored. *See* 740 ILCS 14/15(b).

63.   Likewise, BIPA also requires that entities collecting biometric identifiers publish and make publicly available written retention schedules and guidelines for permanently destroying biometric identifiers collected. *See* 740 ILCS 14/15(c).

III.   Illinois' Biometric Information Privacy Act

64.   BIPA defines biometric identifiers as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10 (emphasis added).

65.   Facial geometry is a permanent, unique biometric identifier associated only with a specific person. Collecting and storing a person's face geometry exposes them to serious and irreversible privacy risks. For example, if a device or database

containing stored images of facial geometry is hacked, breached, or otherwise

compromised, the person has no means by which they can prevent identity theft or

unauthorized hacking of secure devices which use facial recognition to grant access.

66.   Recognizing the need to protect citizens from these risks, Illinois

enacted the Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA") in

2008, to regulate companies that collect and store biometric identifiers, such as facial

geometry. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276.

67.   Accordingly, BIPA makes it unlawful for a company to, *inter alia*,

"collect, capture, purchase, receive through trade, or otherwise obtain a person's or a

customer's biometric identifiers … unless it first:

> 1)   informs the subject . . . in writing that a biometric identifier … is being collected or stored;
>
> 2)   informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier … is being collected, stored, and used; and
>
> 3)   receives a written release executed by the subject of the biometric identifier … or the subject's legally authorized representative."

740 ILCS 14/15(b).

68.   Additionally, Section 15(a) of BIPA requires that entities in possession

of biometric identifiers publish a schedule detailing its retention and destruction

plans concerning the biometric identifiers in its possession.

69.   Section 15(a) of BIPA provides that:

> A private entity in possession of biometric identifiers … must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers … when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.

740 ILCS 14/15(a).

70.   As alleged below, Defendants' practices of collecting, storing, and using delivery drivers' biometric identifiers without informed written consent violated all three prongs of § 15(b) of BIPA. Furthermore, Defendants violate § 15(a) of BIPA by failing to publish and make publicly available any written policy regarding Defendants' schedule and guidelines for retaining and permanently destroying individuals' biometric identifiers.

IV.   Defendants Violate Illinois' Biometric Information Privacy Act

71.   Unbeknownst to Plaintiffs, and in direct violation of § 15(b)(1) of BIPA, Defendants collected, scanned, and then indefinitely stored in an electronic database, Plaintiffs' biometric identifiers when Plaintiffs and Class Members made deliveries to the homes of Defendants' customers who used Defendants' security system. Each time Plaintiffs and Class Members made a delivery to Defendants' customers' homes, Defendants' cameras collected Plaintiffs' face and/or hand geometry and stored the images of Plaintiffs' face and body geometry in an electronic database without ever informing Plaintiffs in writing that it was doing so.

72.   Moreover, in direct violation of §§ 15(b)(2) and 15(b)(3) of BIPA, Defendants never informed Plaintiffs and Class Members who had their biometric identifiers collected, of the specific purpose and length of time for which their biometric identifiers would be collected, stored, and used, nor did Defendants ever obtain a written release.

73.   Finally, and in direct violation of § 15(a) of BIPA, Defendants failed to publish policies for public access identifying its retention schedules or guidelines for permanently destroying any of these biometric identifiers.

<u>**CLASS ALLEGATIONS**</u>

74.   Plaintiffs bring this matter on behalf of themselves and all similarly situated in the following class:

> **Illinois Class:** All natural persons in Illinois who are delivery drivers and who, when making deliveries, had their biometric identifiers

collected, stored, and scanned by eufy cameras and software from November 27, 2018, to present.

75. Excluded from the Class are: (1) any Judge or Magistrate presiding over this action and any members of their families; (2) Defendants, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which Defendants or its parents have a controlling interest and their current or former employees, officers, and directors; and (3) Plaintiffs' counsel and Defendants' counsel.

76. The members of the Class are so numerous that joinder of all members is impracticable. While the exact number of Class members is unknown to Plaintiffs at this time, such information can be ascertained through appropriate discovery from records maintained by Defendants and its agents.

77. Plaintiffs reserve the right to expand, limit, modify, or amend the class definition, including the addition of one or more Subclasses, in connection with their motion for class certification, or at any other time, based on, *inter alia*, changing circumstances and new facts obtained.

78. **Numerosity:** Class Members are so numerous that joinder of all members is impracticable. Plaintiffs believe that there are thousands of delivery drivers who are Class Members described above who have been damaged by Defendants' unlawful collecting, storing, and using of their biometric identifiers.

79. **Commonality and Predominance:** The questions of law and fact common to the class which predominate over any questions which may affect individual class members include, but are not limited to:

    a.   whether Defendants collected or otherwise obtained Plaintiffs' and the Class's biometric identifiers;

    b.   whether Defendants properly informed Plaintiffs and the Class that it collected, used, and stored their biometric identifiers;

    c.   whether Defendants obtained a written release (as defined by 740 ILCS 14/10) to collect, use, and store Plaintiffs' and the Class's biometric identifiers;

d.   whether Defendants developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers when the initial purpose for collecting or obtaining such identifiers has been satisfied or within 3 years of their last interaction, whichever comes first;

e.   whether Defendants destroyed Plaintiffs' and the Class's biometric identifiers once that information was no longer needed for the purpose for which it was originally collected; and

f.   whether Defendants' violations of BIPA were committed intentionally, recklessly, or negligently.

80.   **Typicality:** The claims of the named Plaintiffs are typical of the claims of the Class because the named Plaintiffs, like other members of the Class, made deliveries to customer's homes and had their biometric identifiers collected, stored, and analyzed by Defendants' cameras and software without providing consent, nor did Defendants provide Plaintiffs and Class Members with written policy made publicly available establishing a schedule and procedure for permanently destroying Plaintiffs' and Class Members' biometric identifiers.

81.   **Adequate Representation:** Plaintiffs have retained and are represented by qualified and competent counsel who are highly experienced in complex consumer class action litigation. Plaintiffs and their counsel are committed to vigorously prosecuting this class action. Neither Plaintiffs, nor their counsel, have any interest adverse to, or in conflict with, the interests of the absent members of the Class. Plaintiffs are able to fairly and adequately represent the interests of the Class. Plaintiffs have raised viable statutory claims of the type reasonably expected to be raised by members of the Class and will vigorously pursue those claims. If necessary, Plaintiffs may seek leave of this Court to amend this complaint to include additional Class Representatives to represent the Class or additional claims as may be appropriate.

82.   **Superiority:** A class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual litigation of

the claims of all members of the Class is impracticable. Even if every member of the

Class could afford to pursue individual litigation, the Court system could not. It

would be unduly burdensome to the courts in which individual litigation of

numerous cases would proceed. Individualized litigation would also present the

potential for varying, inconsistent, or contradictory judgments, and would magnify

the delay and expense to all parties and to the court system resulting in multiple trials

of the same factual issues. By contrast, the maintenance of this action as a class

action, with respect to some or all of the issues presented herein, presents fewer

management difficulties, conserves the resources of the parties and of the court

system and protects the rights of each member of the Class. Plaintiffs anticipate no

difficulty in the management of this action as a class action. Class-wide relief is

essential to compel compliance with BIPA.

COUNT I
Violation of 740 ILCS 14/15(b)
(On Behalf of Plaintiffs and the Class)

83.   Plaintiffs incorporate the foregoing allegations as if fully set forth

herein.

84.   BIPA makes it unlawful for any private entity to, among other things,

"collect, capture, purchase, receive through trade, or otherwise obtain a person's or a

customer's biometric identifiers … unless it first: (1) informs the subject . . . in

writing that a biometric identifier … is being collected or stored; (2) informs the

subject . . . in writing of the specific purpose and length of term for which a

biometric identifier … is being collected, stored, and used; and (3) receives a written

release executed by the subject of the biometric identifier or information. . ." 740

ILCS 14/15(b).

85.   Defendants failed to comply with these BIPA mandates.

86.   Fantasia Trading LLC is a limited liability company doing business as

eufy and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

1

2

87.   Anker Innovations Limited is a company doing business as eufy and thus qualifies as a "private entity" under BIPA. *See Id.*

3

4

5

6

7

88.   Plaintiffs and Class Members are delivery drivers in Illinois who had their "biometric identifiers," including scans of face and hand geometry, collected, captured, received, or otherwise obtained by Defendants from video and/or images recorded by a eufy device and scanned by eufy software to differentiate between humans and non-human entrants on the camera-owner's property.

8

9

10

11

89.   Plaintiffs and Class Members' face, body, and hand geometry was stored and mechanically measured to create numerical representations used as "face templates" that can be used to uniquely identify Plaintiffs and Class Members. *See* 740 ILCS 14/10.

12

13

14

15

90.   Defendants collected, captured, or otherwise obtained Plaintiffs' and Class Members' "biometric identifiers" (which it used to create and store uniquely identifying face geometry) without first obtaining signed written releases, as required by 740 ILCS 14/15(b)(3), from any of Plaintiffs.

16

17

91.   Plaintiffs' and Class members' scans of face and/or hand geometry constitute "biometric identifiers." *See* 740 ILCS 14/10.

18

19

20

21

22

92.   Defendants never informed Plaintiffs or members of the Class in writing that their biometric identifiers were being collected, captured, stored, and/or used, nor did Defendants inform Plaintiffs and members of the Class in writing of the length of time for which their biometric identifiers were being collected, stored, and used as required by 740 ILCS 14/15(b)(1)-(2).

23

24

25

26

93.   By collecting, capturing, storing, and/or using Plaintiffs' and members of the Class's biometric identifiers as described herein, Defendants violated Plaintiffs' and the Class's right to privacy in their biometric identifiers as set forth in BIPA. *See* 740 ILCS 14/1, *et seq.*

27

28

94.   And while Plaintiffs and members of the Class are not required to plead that Defendants can link these identifiers back to Plaintiff and Class Members,

1 Defendants are nonetheless able to do so. This is because most people have

2 Facebook, Twitter, Snapchat, or other social media accounts bearing their real-life

3 names and photos. Those real-life names and photos are publicly available to allow

4 other unconnected people to find them. Defendants are capable of employing the

5 very same facial recognition technology used in its cameras and base stations on

6 someone's public facing social media profile to match that individual's biometric

7 identifiers collected from their public online photos to their biometric identifiers

8 collected by its cameras and base station during a home visit. As such, Defendants'

9 human recognition feature is capable identifying an individual.

10   95.   On behalf of themselves and the Class, Plaintiffs seek: (1) declaratory

11 relief; (2) injunctive and equitable relief as is necessary to protect the interest of

12 Plaintiffs and the Class by requiring eufy comply with BIPA's requirements for the

13 collection, storage, and use of "biometric identifiers" as described herein; (3)

14 statutory damages of $1,000.00 pursuant to 740 ILCS 14/20 for each negligent

15 violation of BIPA committed by eufy; (4) statutory damages of $5,000.00 pursuant

16 to 740 ILCS 14/20 for each intentional or reckless violation of BIPA committed by

17 eufy; and (5) reasonable attorneys' fees and costs and other litigation expenses

18 pursuant to 740 ILCS 14/20(3).

<div align="center">

COUNT II
Violation of 740 ILCS 14/15(a)
(On Behalf of Plaintiffs and the Class)

</div>

19

20

21   96.   Plaintiffs incorporate the foregoing allegations as if fully set forth

22 herein.

23   97.   BIPA mandates that companies in possession of biometric data establish

24 and maintain a satisfactory biometric data retention and deletion policy.

25 Specifically, those companies must: (i) make publicly available a written policy

26 establishing a retention schedule and guidelines for permanent deletion of biometric

27 data (at most three years after the company's last interaction with the individual);

28

---

and (ii) actually adhere to that retention schedule and actually delete the biometric identifiers. *See* 740 ILCS 14/15(a).

98.   Defendants failed to comply with these BIPA mandates.

99.   Plaintiffs are individuals who had their "biometric identifiers" captured and/or collected by Defendants, as explained in detail above. *See* 740 ILCS 14/10.

100.   Plaintiffs' biometric identifiers consisted of scans of face geometry, as defined by BIPA. *See* 740 ILCS 14/10.

101.   Defendants failed to provide a publicly available retention schedule or guidelines for permanently destroying Plaintiffs' biometric identifiers as specified by BIPA. *See* 740 ILCS 14/15(a).

102.   On behalf of themselves and the Class, Plaintiffs seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Class by requiring Defendants to comply with BIPA's requirements for the collecting, storing, and using biometric identifiers as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seek judgement against Defendants as follows:

A.   Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiffs as representatives of the Class, and appointing their counsel as Class Counsel of the Class;

B.   Declaring that Defendants' actions, as set out above, violate BIPA, 740 ILCS 14/1, *et seq.*, with respect to Plaintiffs and Class Members;

C.   Awarding statutory damages to Plaintiffs and Class Members of $1,000.00 pursuant to 740 ILCS 14/20(1) for each violation of BIPA

1
2

committed negligently, and $5,000.00 pursuant to 740 ILCS 14/20(2) for each violation of BIPA committed intentionally or recklessly;

3
4
5

D. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and members of the Class, including *inter alia*, an order requiring Defendants to collect, store, and use biometric identifiers in compliance with BIPA;

6

E. Awarding Plaintiffs and the Class their reasonable litigation expenses and attorneys' fees pursuant to BIPA;

7
8

F. Awarding Plaintiffs and the Class pre- and post-judgment interest, to the extent allowable;

9

G. Awarding Plaintiffs and the Class such other and further relief as equity and justice may require.

10

JURY TRIAL DEMANDED

11
12
13
14

Under Federal Rule of Civil Procedure 38, Plaintiffs, individually and on behalf of the members of the Class, exercise their right under the Seventh Amendment to the United States Constitution and demand a trial by jury.

15
16

Dated: August 5, 2024   Respectfully submitted,

17

BURSOR & FISHER, P.A.

18
19

By: /s/ *L. Timothy Fisher*
          L. Timothy Fisher

20
21
22
23
24
25
26

L. Timothy Fisher (State Bar No. 191626)
Stefan Bogdanovich (State Bar No. 324525)
Joshua B. Glatt (State Bar No. 354064)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ltfisher@bursor.com
            sbogdanovich@bursor.com
            jglatt@bursor.com

27
28

Attorneys for Plaintiffs